Exhibit E

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDIA DIVISION

UNITED STATES OF AMERICA, et al., Plaintiffs, v. GOOGLE, LLC, Defendant.	Case No. 1:23-cv-00108 (LMB/JFA) HON. LEONIE H. BRINKEMA

REBUTTAL EXPERT REPORT OF DR. WENKE LEE
Feb 13, 2024

69. In addition, many defenses against digital advertising fraud may benefit from industry collaboration between independent ecosystem components. [redacted] one such example in ads.txt files,[redacted] which prevents domain spoofing through the cooperative implementation of ads.txt files by publishers and the verification by demand partners of the authenticity of domains via those files. The existence of ads.txt as a security standard emphasizes the ability of holistic ecosystem defenses. Indeed, these data-sharing standards and practices and security protocols are open, available, and encouraged to be utilized by independent parties to increase ecosystem cybersecurity. The cybersecurity and anti-fraud industry has long adopted this practice. For example, there are publicly available IP blacklists for anti-spam purposes, e.g., Blacklist Check.[47] As discussed earlier, TLS (transport layer security, formerly SSL) provides essential support for secure network communications, and OpenSSL, an open-source toolkit, is widely used on the Internet including most HTTPS websites.[48]

70. Mr. Ferrante has [redacted]

Paola Spoletini, Mazeiar Salehie, Luca Cavallaro, and Bashar Nuseibeh, "Automating trade-off analysis of security requirements," Requirements Engineering 21, no. 4 (2016): 481–504; Natasha Nelson and Stuart Madnick, "Trade-offs between digital innovation and cyber-security," working paper (2017): 1–31.

[46] [redacted] similar industry-wide files include app-ads.txt, sellers.json, and SellerObjects. These all serve the purpose of verifying and authenticating domains and advertisers to one another.

[47] "Blacklist Check," WhatIsMyIPAddress, accessed February 12, 2024, https://whatismyipaddress.com/blacklist-check. [redacted]

[48] For a history and overview of the OpenSSL protocol, *see* "Open SSL," Wikipedia, accessed February 12, 2024, https://en.wikipedia.org/wiki/OpenSSL#:~:text=It%20is%20widely%20used%20by,the%20majority%20of%20HTTPS%20websites.

learning model for increasing click fraud detection rates that is a combination of two learning models used for feature transformation and classification applied to click fraud datasets.[60] These findings continue to be translatable to industry advancements. For example, Cloudflare, another leading cybersecurity firm, continues to innovate upon such machine learning research and deploy prevention and detection techniques in the market.[61]

Domain Spoofing

83. Domain spoofing is a common type of fraud found in many digital ecosystems including the digital advertising ecosystem.[62] This type of fraud involves faking the domain of a web address by a fraudster to appear to be a legitimate web domain (e.g., a fraudster fakes his domain name to appear as nytimes.com when the fraudster has no relation to the legitimate website). This type of attack has existed since the early days of the internet.[63] In the digital advertising ecosystem, this type of fraud is employed to trick advertisers into displaying ads on a different (one operated by fraudsters) website than intended (the legitimate website). This is an extremely prevalent form of fraud, and as such it is extremely well studied, and has a wide variety of mitigations.[64]

84. A common defense to domain spoofing includes the use of the ads.txt standard outlines by IAB.[65] While the effectiveness of ads.txt in completely preventing domain spoofing is limited by adoption and maintenance of these files, the presence of this standard demonstrably reduces

[60] Thejas G.S., Surya Dheeshjith, S.S. Iyengar, N.R. Sunitha, and Prajwal Badrinath, "A hybrid and effective learning approach for Click Fraud detection," *Machine Learning with Applications* 3, no. 15 (2021): 1–10.

[61] "What is click fraud?," Cloudflare, accessed February 13, 2024, https://www.cloudflare.com/learning/bots/what-is-click-fraud/.

[62] *See e.g.*, S. Maroofi, M. Korczyński, A. Hölzel, and A. Duda, "Adoption of Email Anti-Spoofing Schemes: A Large Scale Analysis," in *IEEE Transactions on Network and Service Management* 18, no. 3 (2021): 3184–3196; Zhijun Wu, Yun Zhang, Yiming Yang, Cheng Liang, and Rusen Liu, "Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey," *IEEE Access* 8 (2020): 165444–165496.

[63] Amir Herzberg and Ahmad Gbara, "Protecting (even) Naïve Web Users, or: Preventing Spoofing and Establishing Credentials of Web Sites," DIMACS Technical Report, May 2004, http://dimacs.rutgers.edu/archive/TechnicalReports/TechReports/2004/2004-23.pdf.

[64] This survey paper examines over 170 peer-reviewed publications that consider attack vectors and mitigations for domain spoofing attacks. Aminollah Khormali, Jeman Park, Hisham Alasmary, Afsah Anwar, Muhammad Saad, and David Mohaisen, "Domain name system security and privacy: A contemporary survey," *Computer Networks* 185 (2021): 1–28.

[65] "Ads.txt," IAB, accessed February 13, 2024, https://www.iab.com/guidelines/ads-txt/.

incidents of domain spoofing attacks in digital advertising.[66] To reiterate from Section IV-C, these files are open for use by *all* parties in the digital advertising ecosystem, and the IAB encourages *all* parties in the digital advertising ecosystem adopt and utilize ads.txt files to reduce incidences of fraud.[67] Since the advent of ads.txt, more anti-domain-spoofing standard files have been proposed and adopted.[68]

85. Cloudflare and Crowdstrike, two leading cybersecurity firms, continue to use industry standards and best practices and build upon this body of academic research, and deploy prevention and detection techniques in the market.[69]

Drive-by Download

86. Drive-by download attacks are another type of fraudulent attack that is common across multiple digital ecosystems. This attack refers to the unintentional download of malicious software onto a user's device. In the digital advertising ecosystem, a drive-by download can occur via a malicious advertisement presented on a web page.[70] Even legitimate websites that do not contain any exploits can contain insecure advertisements that can lead to a drive-by download attack.[71]

87. The academic community has made significant progress in identifying these attacks. Researchers at Victoria University of Wellington published an academic paper detailing a proposed framework for identifying potential features in a webpage that may be exploited for drive-by download attacks. The researchers analyzed state changes that occur in rendered HTML

---

[66] Muhammad Ahmad Bashir, Sajjad Arshad, Engin Kirda, William Robertson, and Christo Wilson, "A Longitudinal Analysis of the ads.txt Standard," in *Proceedings of the Internet Measurement Conference* (2019): 294–307.

[67] "Ads.txt," IAB, accessed on February 13, 2024, https://www.iab.com/guidelines/ads-txt/.

[68] *See, e.g.*, "Sellers.Json," IAB Tech Lab, last modified July 27, 2020, https://iabtechlab.com/sellers-json/; "Authorized Sellers for Apps (app-ads.txt)," IAB Tech Lab, March 2019, https://iabtechlab.com/wp-content/uploads/2019/03/app-ads.txt-v1.0-final-.pdf.

[69] "What is domain spoofing?," Cloudflare, accessed February 12, 2024, https://www.cloudflare.com/learning/ssl/what-is-domain-spoofing/; Bart Lenaerts-Bergman, "What is Domain Spoofing?," Crowdstrike, October 19, 2022, https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/domain-spoofing/.

[70] Niels Provos, Panayiotis Mavrommatis, Moheeb Abu Rajab, and Fabian Monrose, "All Your iFRAMEs Point to Us," in *17th USENIX Security Symposium* (2008): 1–15.

[71] Niels Provos, "Drive-by Downloads via Ads," USENIX, May 13, 2008, https://www.usenix.org/legacy/event/sec08/tech/full_papers/provos/provos_html/node11.html.

because Google prevented certain instances of fraud, it does not mean other SSPs and DSPs did not prevent just as much if not more fraud using their own in-house or third-party tools.

Wenke Lee, Ph.D

Feb 13, 2023
Date